8 January 1999

Proceedings

November 18, 1998 meeting
Forum on Privacy and Security in Healthcare

Sponsors:

National Information Assurance Partnership (NIAP)
Healthcare Open Systems & Trials (HOST)

Contributing Scribes:

Paul J. Brusil, Ph. D (NIAP)
Edwin F. Steeble (NIAP/NSA)
Victoria Thompson (Arca Systems)

Editors:

Arnold Johnson (NIAP/NIST)
Lewis Lorton, DDS, MSD (HOST)

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 08011999	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Proceedings November 18, 1998 meeting Forum on Privacy and Security in Healthcare	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) National Information Assurance Partnership (NIAP)	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 25	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	1/8/99	Report

4. TITLE AND SUBTITLE
November 18, 1998 meeting Forum on Privacy and Security in Healthcare

5. FUNDING NUMBERS

6. AUTHOR(S)
Arnold Johnson, Lewis Lorton

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

Staff and management of the National Information Assurance Partnership (NIAP) and the Healthcare Open Systems & Trials (HOST) consortium sponsored a one day workshop for the purpose of collectively examining whether there was interest in establishing a Forum on Privacy and Security in Healthcare (the “Forum”). Workshop attendees included a diverse set of healthcare-related individuals with diverse interests, intentions and backgrounds about security. The proposed purpose of the Forum would be to address healthcare community IT security needs by providing tools for translating healthcare security policy into standard security requirements that could be used as the basis for assessing healthcare IT products’ compliance to mandated healthcare policies. Many participants concurred that implementing IT-related healthcare policy was a significant problem, especially in light of general perceptions that such policy is often very difficult to translate into real terms. Policy at the federal level is often written without the inputs of IT and security technologists/implementors. Determining whether a product or system of products complies with such policy was perceived to be an equally challenging task. With these problems as a back drop, high level

14. SUBJECT TERMS
IT, Healthcare Security

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

Executive Summary

Staff and management of the National Information Assurance Partnership (NIAP) and the Healthcare Open Systems & Trials (HOST) consortium sponsored a one day workshop for the purpose of collectively examining whether there was interest in establishing a Forum on Privacy and Security in Healthcare (the "Forum"). Workshop attendees included a diverse set of healthcare-related individuals with diverse interests, intentions and backgrounds about security.

The proposed purpose of the Forum would be to address healthcare community IT security needs by providing tools for translating healthcare security policy into standard security requirements that could be used as the basis for assessing healthcare IT products' compliance to mandated healthcare policies.

Many participants concurred that implementing IT-related healthcare policy was a significant problem, especially in light of general perceptions that such policy is often very difficult to translate into real terms. Policy at the federal level is often written without the inputs of IT and security technologists/implementors. Determining whether a product or system of products complies with such policy was perceived to be an equally challenging task.

With these problems as a back-drop, high-level education was provided to workshop attendees about:

- a new set of ISO security-relevant standards called the Common Criteria (CC),
- what tools exist to cast policy into CC-based profiles -- so-called Protection Profiles (PPs) – of product or procurement requirements,
- the Common Criteria Evaluation and Validation Scheme (CCEVS) – the US plan for providing independent assessment and verification of product compliance with standard security specifications, and
- why the healthcare community should participate in a process for capturing security requirements, especially policy-driven requirements.

Also, an overview of a plan for community-based PP development was given.

While there was near-unanimous agreement that the general notion of a Forum was good and that the general problem space it would likely address is significant, there were also concerns. There were several concerns expressed:

- the specific niche to be filled by such a Forum was not yet well-formed;
- others in the community needed to be made aware and needed to buy in; and

- there needed to be a clearer, more compelling, business/economic case made to attract on-going participants and to increase the likelihood for success.

It was noted that while the meeting had heterogeneous representation spanning a number of different healthcare-related organizations, several other pertinent organizations and healthcare sectors were absent.

Riding the demonstrated enthusiasm, it was decided to establish an email exploder to continue discussions in real time and to organize a follow-up meeting. Interim discussions would focus on

- identifying other pertinent organizations who are working in this space and who should be at the table,

- honing concepts for the Forum's niche,

- honing what specific topics and working groups need to be established.

It was thought that the follow-up meeting – perhaps one attached to a large extant healthcare conference - should include:

- presentations from other related, significant organizations in order to get a more comprehensive picture of work that is related and may need to be coordinated, and

- a worked example of translating exemplar healthcare policy to security architecture and to PPs.

This document is the proceedings that have emerged summarizing the activities and discussions at the Forum organizational workshop. This document is being made available to all participants at, and registrants for, this meeting. This document is also being made available to any party interested in improving the confidence that security requirements for information technology used by the healthcare community are understandable and appropriate, and that security-enhanced information technology products and systems for the healthcare community adequately implement security requirements. These proceedings are freely distributable to anyone.

Table of Contents

NOTE: The last two pages of this document provide URLs to download Appendix A through L. Most of these files are Microsoft Powerpoint presentations.

Introduction

On 18 November 1998, the National Information Assurance Partnership (NIAP) and the Healthcare Open Systems & Trials (HOST) consortium, with the support of ARCA Systems, Inc. (a HOST member), sponsored an open meeting of individuals from a number of organizations related to the healthcare, security and information technology (IT) communities.

The purpose of the meeting, as stated in the invitational electronic mail messages, was to develop an industry Forum on IT security in healthcare. In preparation for the meeting it was suggested that attendees review the potential government regulations on healthcare that appeared in the Federal Register: August 12, 1998 (Volume 63, Number 155) [Page 43241-43280] from the Federal Register Online via GPO Access [wais.access.gpo.gov] [DOCID:fr12au98-28].

Arnold Johnson, NIAP Program Manager at NIST (National Institute of Standards and Technology), opened the meeting by providing background on the sponsoring organizations.

The purpose of NIAP is to increase the quality of commercially produced IT products that are security-enhanced. Details about NIAP's initiatives appear on the NIAP web site (http://niap.nist.gov).

HOST is a nonprofit consortium whose mission is to promote the development of IT to improve healthcare. Details about HOST appear on its web site (http://www.hostnet.org).

Mr. Johnson noted that the combined, intersecting strengths and interests of HOST and NIAP are clearly appropriate to address the needs of security-enhanced IT for healthcare.

Dr. Lewis Lorton, HOST Executive Director, provided introduction and motivation for the meeting (see Appendix C). Dr. Lorton opened by reminding attendees that the public, as patients, is very interested in the privacy and security of their medical data, and, accordingly, there was need to energize and to focus healthcare industry responses to the public's concern. This is especially timely given the exploding number of policies and regulations being developed pertinent to healthcare IT security and the burgeoning need to be able to show due diligence by assessing compliance of security-enhanced IT products to such policies and regulations. Given the impact of such policies and regulations to all in the healthcare field, there is need to provide a public environment to foster discussions and to develop solutions that bridge the gap between policies/regulations and IT products/systems.

Dr. Lorton reviewed the agenda (see Appendix A) for the remainder of the meeting. The presentations were geared to provide a basic primer about IT security for the healthcare field. Some initial concepts and examples would be given about (a) defining security requirements using tools and techniques provided by a new international standard, (b) developing security architectures, and (c) using an emerging, internationally-recognized methodology for evaluating the quality of IT products that include implementations of

security. Also, initial concepts would be given about convening a cross-industry effort to provide a foundation for healthcare IT security quality. This foundation would be based on efforts to organize and specify healthcare IT security requirements according to standards that facilitate independent evaluation and validation of products. Dr. Lorton made it clear that the continuation and direction of this activity will be decided by these attendees and other interested parties who become involved and contribute.

A total of 56 individuals participated in the meeting and a total of 135 asked to be kept on the mailing list. The list of individuals who participated or registered appears in Appendix B.

Overview of Formal Presentations

Healthcare Security: Problem Statement. The first formal presentation, "Healthcare Security: Problem Statement", was given by Victoria Thompson of ARCA Systems, Inc. A copy of the presentation appears in Appendix D. Ms. Thompson's talk focused on specification of the problem, the needs of the stakeholders who are impacted by the problem, and a potential solution to the problem.

The essence of the problem is that, for a variety of reasons, numerous healthcare-related organizations need a method to express healthcare IT security requirements that arise from various organizational and governmental rules, policies and legislation. These same organizations also need to verify products' compliance with stated security requirements. The primary stakeholders that are impacted are the owners and users of healthcare information. There are many secondary stakeholders.

The proposed solution is based on:

a) developing a healthcare security architecture (along the lines of the subsequent presentation appearing in Appendix F),
b) developing Common Criteria protection profiles (as described in Appendix E) that specify various piece-parts of security requirements from within the healthcare-specific security architecture, and
c) evaluating healthcare IT security products (along the lines of the subsequent presentation appearing in Appendix G) to ensure that security requirements are met by products.

The presentation precipitated questions and discussion. It was noted that lawmakers in this area are at a big disadvantage. Legislators want comprehensive law; but legislation and regulation usually does not reflect sufficient detail and technical 'best practices." Legislative staff who draft laws are not necessarily experts in the field. They do not typically get technology inputs, nor do they usually get feedback about the implementability of solutions. For example, the HHS (Health & Human Services) NPRM (Notice of Proposed Rule Making) implied certain security requirements that could not be implemented because techno-policy issues were not delineated. There were over 1300 non-specific, generic comments on the draft of this document and very little of this feedback came from technologists.

Introduction to the Common Criteria for IT Security. The next formal presentation, "Introduction to the Common Criteria for IT Security", was given by Gene Troy of NIST. A copy of the presentation appears in Appendix E.

This presentation provided motivation and general information about the Common Criteria (CC) and Common Evaluation Methodology (CEM) standards. These standards were developed because of the need to provide a generic, flexible means for specifying any type of IT security need or product, and to test and evaluate products in a well understood way

in order to gain confidence in such products. The parts of the CC standard were briefly described, along with the notions of security requirements specified either as user-driven protection profiles (PPs) or product-driven security targets (STs). A "bird's eye" overview of the CEM was also provided. A white paper, "Common Criteria: Launching the International Standard", was made available [Ref. 3]. This paper provides more details about the purpose and usage of the CC, and the relationship of the CC to multi-national, mutual recognition agreements to accept the results of CC/CEM-based security evaluations across national borders.

Some questions and comments were stimulated by the presentation. It was noted that certain healthcare IT systems such as patient record systems and hospital business application systems (collectively known as Enterprise Resource Planning [ERP] systems) such as those pertaining to human resources, payroll, inventory, service delivery/scheduling, etc. are expected to require moderate levels of security assurance. A CC Evaluation Assurance Level (EAL) of 3 or 4 will likely be appropriate for such systems. Embedded systems such as drug metering systems and other smaller systems are candidates for higher security assurance levels such as EAL 5 or EAL6. In some senses, smaller systems are "easier" to test and evaluate compared to larger systems because there are fewer aspects of the system that need to be evaluated and analyzed.

One attendee had the misimpression that very few CC-based PPs existed or were possible and that only one PP was being proposed for the entirety of security requirements in the healthcare field. It was made clear that there is absolutely no notion of just a single PP for the entirety of healthcare's security needs. Rather, it is expected that there will be a plethora of PPs and STs applicable (a) to very diverse healthcare scenarios that depend on secure IT and (b) to very diverse sets of security-enhanced products and systems.

Developing a Security Architecture – From Policy to Systems Implementation. The next formal presentation, "Developing a Security Architecture – From Policy to Systems Implementation", was given by Ron Ross of NIAP/NIST. A copy of the presentation appears in Appendix F.

This presentation provided information about tools that are available for supporting the acquisition process from its start as top-level healthcare policy down to the level of products being implemented to comply with policy-level security requirements. There is a crucial need to develop a security architecture that can drive the development of, and be coupled with, PPs so that comprehensive IT security requirements for healthcare systems can be specified. The security architecture provides the roadmap from policy to product implementation. It allows the balancing of technical/product and non-technical/procedural solutions to aspects of security needs and objectives stated in top-level policy.

Developing a security architecture is a process to help organize thinking about security requirements and to break down healthcare systems with complex security needs into more understandable, elementary elements of security requirements. In so doing, it is possible that generalized, consumer-driven, security requirements for healthcare systems can be decomposed into a set of more elementary, technology-specific PPs (such as O/S

PPs, DBMS PPs, Firewall PPs, etc.) so that products claiming conformance to such elementary PPs can be procured and integrated to form the more complex, overall healthcare system.

Common Criteria Evaluation and Validation Scheme – An Overview and Conceptual Framework. The next formal presentation, "Common Criteria Evaluation and Validation Scheme – An Overview and Conceptual Framework", was given by Ron Ross of NIAP/NIST. A copy of the presentation appears in Appendix G.

This presentation summarized NIAP's framework (a.k.a. "scheme") for testing and evaluating security-enhanced IT products within the US. Key to the scheme is NIAP's commitment to providing (a) independent government accreditation of commercial, testing and evaluation facilities, as well as (b) independent government validation of testing and evaluation results obtained by accredited laboratories. Testing and evaluation help consumers compare capabilities and limitations of products. Validation can be thought of as a second level of increased assurance/confidence about products.

NIAP validation of the product testing and evaluation results culminates in the award of a CC certificate to the vendor. The certificate is recognized within the several countries that are partaking in a "mutual recognition arrangement" in which products built and tested in any country can be bought with confidence and no further testing in any other country.

Questions about the time duration to complete tests and evaluations were stimulated by the presentation. It was noted that evaluations of products claiming EAL2 assurance (a low level of assurance) were averaging about 60-90 days. Products claiming higher assurance levels take longer because of the increased number of security assurance requirements that needed to be evaluated. For example, although there are fewer completed examples, it appears that EAL4 level evaluations are taking 5-6 months. There was also discussion about the needs for rapid, cost-effective, evaluation maintenance processes to keep CC certificates alive as products go through revisions and minor updates.

Community Contributions to Healthcare Protection Profiles: What? And Why? The next formal presentation, "Community Contributions to Healthcare Protection Profiles: What? And Why?" was given by Diann Carpenter of ARCA Systems. A copy of the presentation appears in Appendix H.

The speaker provided pragmatic information and motivation regarding the PP content areas that would best benefit from collaborative efforts among healthcare community users and other healthcare secure IT stake-holders in concert with security experts. Healthcare users are crucial to identifying the purpose, scope and objectives of security, as well as any environmental considerations and legacy systems that may need to be incorporated as constraints/assumptions impacting community-driven PPs. Security experts are key to using the CC to select and aggregate requisite accompanying CC security requirements to be incorporated into community-developed PPs.

Healthcare Security Forum Demonstration Project. The next formal presentation, "Healthcare Security Forum Demonstration Project", was also given by Diann Carpenter of ARCA Systems. A copy of the presentation appears in Appendix I.

This presentation proposed that a demonstration project be established for the purpose of prototyping how community collaboration can be brought to bear to develop a PP or some sort of starter set of related PPs for some aspect of the healthcare community. It was noted that NIAP was looking into the possibility of providing some seed money for a demonstration project. The initiation of such a project is pending a community decision to proceed.

Protection Profiles for Healthcare Internet. The next formal presentation: "Protection Profiles for Healthcare Internet" was given by Jon 'JB' Barmettler of SAIC Health Care. A copy of the presentation appears in Appendix J.

A tri-state federation (Massachusetts, Minnesota, Washington) commissioned SAIC to develop a description of security requirements for health data on the Internet. This presentation summarized a specific vendor's solution to this three state project [Ref. 1, 2]. focused on prototyping a solution for the problem of managing security and risk for electronic healthcare data when such data are transported over the Internet. Various profiles of healthcare security, so-called HSLs (Healthcare Security Levels) were defined. HSL levels provide additive security services. That is, higher numbered levels add additional security features (as well as additional cost and risk mitigation) to lower numbered levels.

Eight levels were defined ranging from (a) those with minimal security capabilities such as minimally encrypted mail for transporting patient data and a commonly-agreed certificate authority, to (b) mid-levels that add role-based security and directory services, to (c) high levels that add virtual private networking services and non-repudiation capabilities. While the security services defined in HSLs do not necessarily map precisely to CC security requirements, the underlying notions associated with HSLs can be somewhat likened to CC-style PPs.

A number of diverse questions and comments were triggered to clarify how the work relates to existing standards (such as the emerging CORBAmed Healthcare Resources Access Control [HRAC] security standard), how the HSL profiles relate to PPs, whether there were any operational pilots based on the presented models, how issues about integrating diverse certification authorities (CAs) serving different healthcare domains should be resolved, and so on.

In response, it was noted that lack of project time and funding prevented considering how to utilize the CORBAmed HRAC. Similarly, the notion of PPs was not precisely considered. Indeed, unlike PPs, HSLs are focused strictly on specifying security functionality; HSLs do not specify security assurance requirements like PPs do.

It was noted that several types of PPs could be developed or utilized using the HSLs as starting points. For example, HSLs can point to various different Firewall PPs, CA-server PPs, Role-based Access Control PPs, and so on. It was noted that one state has an operational pilot based on a high level (HSL-6) profile[1], that two other states are joining the Three-State Project, and that more pilots are being planned. It was also noted that states appear to be leaning to the notion of mandating a single, common CA - especially if extant, individual CAs do not come to some consensus on common CA policies.

Healthcare Security Forum Structure. The closing presentation of the morning session: "Healthcare Security Forum Structure" was given by Victoria Thompson of ARCA Systems. A copy of the presentation appears in Appendix K.

This speaker proposed a candidate structure and candidate set of activities for a multi-disciplinary Forum. This Forum would function, in part, as a mechanism for facilitating community-wide participation in the identification of, scheduling and strategic management of, and development of security architectures and PPs of maximal interest to the healthcare community. It was noted that Forum efforts could progress in parallel along both a top-down fashion (in which security architecture work and PP taxonomy work could be focused) and a bottom-up fashion (in which PPs of significant community interest could be developed while top-down work progressed).

The types of personnel that could benefit Forum efforts were identified. To maximize effectiveness, Forum efforts should leverage existing and completed efforts in other market sectors that have defined security architectures and PPs.

Issues were identified regarding the funding of a Forum community effort and the need to provide some sort of minimal organizational infrastructure for such community efforts.

A number of questions and comments arose as workshop attendees began reflecting upon all the formal presentations. A common thread was the issue as to what other organizations and groups need to buy into these organizational efforts in order for there to be success. It was noted that the candidate Forum efforts looked like some sort of standardization effort and that there are several existing healthcare industry standards bodies (such as ASTN [American Society for Testing and Materials], HL7 [Health Level 7], CORBAmed) with which coordination may be useful. It was observed that there were only a handful of vendors at this meeting and that vendors were key to gaining acceptance of a CC-based specification and evaluation strategy in the marketplace.

---

[1] The Privacy and Security Work Group of CHITA (Community Health Information Technology Alliance), an alliance of about 60 health care organizations in the Pacific Northwest, is currently implementing a pilot project to demonstrate secure messaging using the Internet. The project is being done in collaboration with The Agora Group composed of technology security professionals from 150-plus corporations (e.g. Microsoft, Boeing, Nordstrom, Premera Blue Cross, Regence Blue Shield, etc.) and more than 50 federal, state, local and provincial (Canadian) agencies (e.g., U.S. Customs Service, FBI, Secret Service, Seattle Police Department, Canadian Mounted Police).

It was also noted that there are some groups (such as [American Dental Association] and HISB [Health Informatics Standards Board]) that apparently may be doing bits and pieces of integrating people and groups within the healthcare industry. It was therefore wondered whether there might be existing groups with which the proposed Forum efforts might compete. To address these concerns it was suggested that a bigger group be gathered at the next meeting, with more diverse participation from all impacted by a transition to a CC-based specification and evaluation strategy.

The presenter concluded that, unless a significant fraction of the healthcare industry could be enlisted or become contributors/collaborators, there was no need to proceed with the idea of establishing a Forum. It was also made clear that PP development work did not have to be tied to or initiated at the beginning of virgin security requirements development efforts. PP development could be done after requirements efforts are completed or even after products exist.

Overview of Break-out Groups

Three break-out groups were formed with the intent of discussing different topics extracted from the Three-State healthcare security project report [Ref. 1]. The discussion topics identified included: (a-d are Word documents that can be viewed)

(a) Validation of Users, Transactions and Activities (103,424 bytes)
http://niap.nist.gov/11-98FPSH/1validation_roles.doc

(b) Philosophy and Objectives of Protection Activities (46,592 bytes)
http://niap.nist.gov/11-98FPSH/2philosophy_protection.doc

(c) Policy Issues (49,664 bytes)
http://niap.nist.gov/11-98FPSH/3policies.doc

(d) Breakout Groups Mission (116,224 bytes)
http://niap.nist.gov/11-98FPSH/Breakout_Groups_Mission.doc

The break-out groups tended to stray from their appointed discussion topics. Synopses of the various groups' discussions appear below.

Breakout Group 1

Facilitator: Dr. Ron Ross, NIAP
Scribe: Dr. Paul Brusil, NIAP

This discussion group focused on surveying attendees opinions about whether the notion of a Forum on Privacy and Security in Healthcare was useful and in the right direction, and whether the notion of a companion PP demonstration project was useful. The overwhelming theme expressed was that the notion and objectives of a Forum, of PPs based on use of CC technology, and commercial evaluation of products were "great, but …". Specific exemplar points made by attendees are given below regarding (a) the purposes of the Forum, (b) the need to involve other organizations, (c) difficulties in pursuing a top-down approach, and (d) a demonstration project.

Specific to the topic of convening a Forum, all participants thought without any reservations that such a group was needed. Some attendees stressed that the proposed Forum would be useful as a "Knowledge Center" or an "awareness-focusing group" which can serve as a community focal point for maintaining, sharing and disseminating knowledge about healthcare IT security. Accordingly, it was offered that such a group would be useful to help the community figure out how protection profiles would affect users and how PPs could be utilized within the community.

Other attendees also thought the Forum would be a central organization for developing, or coordinating the development of, protection profiles. Some thought that it would be useful to have a central organization (akin to the Internet Engineering Task Force) whose PP

outputs could become widely recognized as practical, community-supported standards. Indeed, one of the attendees who helped to draft HIPA [Health Insurance Portability Act] legislation in this area supported the notion of the Forum in that the framers of such legislation assumed that groups like the proposed Forum would form to act as catalysts to foster the development of solutions for healthcare IT security.

Many participants echoed a concern that several more groups working in the healthcare IT security space (and related spaces) needed to "buy-in" to the notion of PPs. All such groups would have to share any related work accomplished to date in order to prevent rehashing of such previous work, and to otherwise provide inputs to any community-wide PP development efforts. Some of the groups identified included HCR, the National Library of Medicine (NLM), and the G7 (Global 7) international healthcare security group.

It was also noted that several other classes of healthcare and healthcare-related individuals, such as medical practitioners, healthcare organization chief information officers (CIOs) and insurance company CIOs, needed to become involved in these efforts. One attendee indicated that often as many as 200 different organizations touch a patient's medical record; and, many (but not all) of these people and the organizations they represent may need to provide their inputs. At a minimum, data owners' inputs would be essential. The thought of many was that a fair amount of coordination would need to take place before any technical PP development work could begin.

Regarding the topic of establishing an approach for, and developing, protection profiles, all participants thought the notion of developing PPs was essential, but some recognized that difficulties may be encountered. For example, it was pointed out that a top-down approach based on scoping out a security architecture and identifying, a-priori, an appropriate taxonomy of PPs will be hard. There could be several matters that complicate such a top-down approach, e.g.,

- the lack of understandability of legislative and organizational policies which can cause difficulty in recasting policies into classes of PPs,
- different risk/threat assumptions by different organizations,
- the rapid pace of new IT introduction, and
- the business of how to deal with (sometimes rapidly changing) installed bases of legacy systems, especially when different users/consumers have different, legacy-filled environments.

Such matters can impact the development of PPs in that, e.g., different assumptions may need to be made within PPs about what security aspects may be handled by the environment external to the PP. It was also noted that development of PPs to characterize larger systems of integrated/interacting devices will be difficult.

Furthermore, with the rapid changes in underlying technology it was thought that any meaningful security architecture needed to be an information-driven architecture, perhaps based on higher, business-level models of healthcare, and not a technology-driven architecture.

One attendee wondered whether such concerns might impact how/whether vendors support a CC-based approach, even if it is seemingly community-driven. Another attendee added that punitive measures needed to be added to legislation and policies in order for the community to become serious and to prevent a plethora of "experiments in healthcare technology".

Regarding the topic of a demonstration project, many attendees thought that a demonstration or prototyping project would be extremely useful. Some attendees thought that an initial Forum demonstration project focus could be based on some specific scenario from the Three-State project ([Ref. 1], Appendix J).

Others thought that the Three-State project might present too large a demonstration project or that this project was not universally acclaimed. These attendees thought that the initial Forum PP development focus should start with a practical scenario in a narrow area such as the radiation lab or pharmacy areas in which today's IT security requirements might be easier to ascertain than in some broader area of healthcare. Cross-fertilizing the IT security needs of such smaller, perhaps more "stove-pipe-like", constituency groups might be easier than to try to tackle definition of the multi-environmental security needs of some bigger aggregate of the healthcare community. However, there was concern that users typically don't know what their requirements are and instead rely on vendors to tell them what products are available for purchase.

Breakout Group 2

Facilitator: Gary Grossman, Arca Systems
Scribe: Victoria Thompson, Arca Systems

Rather than discussing the prepared questions, this group talked generally about the genesis of HIPA legislation and the various pressures that will ultimately drive implementation. Increasing customer demand was identified as the key driver: if customers see that some technological solution is available, they will begin to demand it and vendors will respond. The group was very interested in the possibilities offered by CC protection profiles and evaluation, but expressed the need for a better understanding of the relationship between architecture, security targets, targets of evaluation and protection profiles in order to see how the initiative proposed by the Forum could benefit them. Involvement by all segments of the community was deemed to be essential.

Breakout Group 3– Policy Issues

Facilitator: Kris Britton, NIAP
Scribe: Edwin Steeble, NIAP

This discussion group started with only five members but grew to eight by the end of the session. The facilitator opened the session by going around the room asking all

participants to introduce themselves and to state why they were here or what they expected. Two people came here to find out, "Who owns the medical records?" Is it the patient, the doctor, or the facility? That turned out to be a excellent question which sparked discussion which led the group to make some other points.

The points were:

(a) State laws, as well as federal laws, effect access.

(b) There are contracts between hospitals and physicians.

(c) Remember to consider internet email when discussing patients records.

(d) Include privacy advocates as well as security advocates when formulating a solution.

(e) Develop a security policy.

(f) Need for patients bill of rights.

(g) Need architectural documents or framework from which to specify products for a system.

Closing Plenary Session

The discussion leaders in the three parallel break-out sessions provided synopses of discussions within their individual break-out groups.

Arnold Johnson provided the closing presentation in which he indicated that both NIAP and NIST resources will also be brought to the table should the community desire to initiate a PP development demonstration project as suggested earlier in the presentation entitled: ""Healthcare Security Forum Demonstration Project". The tabulation of NIAP and NIST resources appears in Appendix L.

Lewis Lorton recapped significant points of the workshop and highlighted future action items arising from the meeting.

The following action items were agreed to be pursued:

1. establish an email exploder to facility discussions and distributions of materials,

2. seek attendees' suggestions about what would be useful working groups within the Forum and what their charters/missions might be,

3. seek attendees' insights about

    (a) what other people and/or organizations are currently doing work related to healthcare security, policy, etc.,

    (b) who would be essential to have at the table at the next Forum meeting, and

    (c) who might be able to brief the status/scope of the organizations they represent,

4. seek attendees' suggestions as to what is the niche that the candidate Forum should fill and what value the Forum should look to provide, and

5. seek attendees' inputs regarding citations for any documents or materials that are believed to be pertinent to this effort.

Follow-on Organizational Meeting

A follow-on meeting was held at the NIAP Conference Center on November 19, 1998. During this meeting, it was stressed that one of the main lessons learned from the November 18, 1999 kick-off meeting was the need to articulate the niche that the proposed Forum on Privacy and Security in Healthcare should fill.

Potential areas of concentration include providing a focal point for

(1) continuing discussions about the use of testing, evaluation and validation as a way to provide confidence that products meet the security requirements mandated by legislation,

(2) leading and coordinating community efforts to specify security requirements in ways to promote cost-effective testing, evaluation and validation of products claiming compliance to mandated security requirements,

(3) stimulating community-wide involvement in pertinent legislation being developed so that such legislation is written in a way to maximize the understandability of security requirements and to maximize the confidence that such requirements can be met by implementable products, and

(4) rallying the community to participate in Forum efforts because of demonstrable payback in participating.

The obvious was noted: that for any healthcare IT security Forum to be successful required the appropriate mix and active participation of a variety of people; and, that the aggregate knowledge base of such participants required multi-disciplinary expertise in the areas of healthcare, IT and security. Potential participants not well represented in the kick-off meeting on November 18, 1998 include payers, providers, administrators, CIOs, CSOs (Chief Security Officers), auditors, various standards organizations, various consortia developing healthcare IT solutions, various other organizations that purportedly are trying to be focal points for collecting healthcare IT requirements, etc.

It was thought that a second workshop was needed to mobilize the requisite candidate participants and to continue organizational efforts for such a multi-disciplinary Forum. An appropriate focus for the second workshop would be to provide a “healthcare security summit” in which all relevant parties in the community could exchange information about what security-related activities each such organization was pursuing or contemplating. A number of potential organizations that should be invited to the second workshop were mentioned.

Logistically, it was thought there might be merit in holding such a second workshop in conjunction with a large, recognized, general symposium. Three such symposia are

scheduled before the end of 2Q99. Pragmatically, it was thought that a second workshop couldn't be organized before February 1999 at the earliest. Of note as a potential venue for the workshop was the HIMSS (Health Information and Management Systems Society) symposium that will be taking place at the end of February in Atlanta. It was noted that the new email exploder (that was created from the list of registrants and attendees to the November 18 workshop) should be used to solicit workers to get involved in organizing the second workshop and to help develop its agenda.

One of the important goals for the second workshop, as well as any earlier community outreach efforts is to develop a simple example that demonstrates our claims made at the first workshop that healthcare policy can be translated into Common Criteria protection profiles (that can subsequently be used as the basis for testing, evaluating and validating products claiming compliance to such policy). Potential policy-based protection profiles that could be developed might be based on an emergency room scenario or some role-based primary care physician scenario.

Preliminary discussions also took place regarding what kinds of working groups might be needed within the Forum if it were to be convened. It was thought that there were needs for at least three working groups:

(a) a policy and legislation working group,

(b) a community awareness and coordination working group, and

(c) one (and eventually many more) practical applications working group.

The purpose of the first working group would be to identify and synopsize existing or emerging policies, laws and regulations pertaining to security and healthcare IT, and to identify and track related legislative efforts.

The purpose of the second working group would be to identify what organizations are working in areas related to security for healthcare IT, to identify work programs and existing products of such organizations, to identify gaps and overlaps among efforts by such groups and the Forum, and to establish liaisons with appropriate groups in order to coordinate appropriate inter-organizational activities and to influence intra-organizational activities.

The purpose of the third working group would be to perform the detailed work of deriving an exemplar protection profile (PP) from specific healthcare security policy and to develop and maintain a security architecture applicable across the healthcare community. It would be envisioned that over time several sub working groups would be temporarily brought into existence to develop, or to coordinate the development of, other specific PPs of broad interest.

It was thought that one of the first discussions to be stimulated on the email exploder should be focused on examining what would be an appropriate mix of initial Forum working groups. Examples of the issues to be discussed include the following. Is the above candidate list of working groups appropriate? Is this too many/too little, or are there needs for completely other working groups that would be more important? Are their proposed purposes understandable and/or useful? Should their missions be different?

Acknowledgments

Thanks are given to all those who have contributed work and work products towards making this meeting happen:

(1) HOST and NIAP senior staff for interest, effort and enormous experience

(2) Arca Systems senior staff for intelligent planning, insight and innumerable hours of effort, and

(3) Minnesota Health Data Institute
Massachusetts Health Data Consortium
Foundation for Health Care Quality
for generously allowing use of their ground-breaking work in this arena.

References

[**Ref. 1**] "A Three-State Health Information Planning Project: Security and Risk Management for Business-to-Business Health Information Networks", developed collaboratively by The Foundation for Health Care Quality, the Massachusetts Health Data Consortium, and the Minnesota Health Data Institute, with the assistance of Science Applications International Corp., June 1998.

[**Ref. 2**] "The Three-State Model Security Plan", available at: http://www.chita.org

[**Ref. 3**] "Common Criteria: Launching the International Standard", by Gene Troy, ITL Bulletin, November 1998, available at: http://csrc.nist.gov/cc/info/cc_bulletin.htm

Appendices

Appendix A: Agenda
Microsoft Word '97 (115,200 bytes)
(http://niap.nist.gov/11-98FPSH/1118_AGENDA1.doc)

Appendix B: List of Registrants and Attendees
(http://niap.nist.gov/11-98FPSH/1118attendance.html)

Appendix C: "Healthcare Security Forum"
by Lewis Lorton
Microsoft Powerpoint (130,048 bytes)
(http://niap.nist.gov/11-98FPSH/ppt/HSF2_IntroLLorton_presentation1.ppt)

Appendix D: "Healthcare Security: Problem Statement"
by Victoria Thompson
Microsoft Powerpoint (87,552 bytes)
(http://niap.nist.gov/11-98FPSH/ppt/HSF3_ProblemStmt_VThompson.ppt)

Appendix E: "Introduction to the Common Criteria for IT Security"
by Gene Troy
Microsoft Powerpoint (82,432 bytes)
(http://niap.nist.gov/11-98FPSH/ppt/HSF4_CommonCriteria_GTroy.ppt)

Appendix F: "Developing a Security Architecture – From Policy to Systems Implementation"
by Ron Ross
Microsoft Powerpoint (268,288 bytes)
(http://niap.nist.gov/11-98FPSH/ppt/HSF5_SecurityArchitecture_RRoss.ppt)

Appendix G: "Common Criteria Evaluation and Validation Scheme – An Overview and Conceptual Framework"
by Ron Ross
Microsoft Powerpoint (253,440 bytes)
(http://niap.nist.gov/11-98FPSH/ppt/HSF6_CCEVScheme_RRoss.ppt)

Appendix H: "Community Contributions to Healthcare Protection Profiles: What? And Why?"
by Diann Carpenter
Microsoft Powerpoint (80,384 bytes)
(http://niap.nist.gov/11-98FPSH/ppt/HSF7_PPcontributions_DCarpenter.ppt)

Appendix I: "Healthcare Security Forum Demonstration Project"
by Diann Carpenter
Microsoft Powerpoint (72,192 bytes)
(http://niap.nist.gov/11-98FPSH/ppt/HSF10_DemoProject_DCarpenter.ppt)

Appendix J: "Protection Profiles for Healthcare Internet"
by JB Barmettler
Microsoft Powerpoint (881,664 bytes)
(http://niap.nist.gov/11-98FPSH/ppt/HSF8_WorkEx_JBBarmettlerSAIC.ppt)

Appendix K: "Healthcare Security Forum Structure"
by Victoria Thompson
Microsoft Powerpoint (91,136 bytes)
(http://niap.nist.gov/11-98FPSH/ppt/HSF9_ProjStructure_VThompson.ppt)

Appendix L: "NIAP/NIST Resources/Services"
by Arnold Johnson
Microsoft Powerpoint (141,824 bytes)
(http://niap.nist.gov/11-98FPSH/ppt/HSF1_OpenRemarksAJv13.ppt)